

04/11/97

PATENT APPLICATION  
ATTANT COMMISSIONER FOR PATENTS  
Washington, D.C. 20231

Case Docket No.: 647

9665 U.S. PTO  
08835749  
04/11/97

Sir:  
Transmitted herewith for filing is the patent application of  
Applicants: Daniel Mendez et al.  
Title: System and Method for Securely Synchronizing Multiple Copies of a Workspace Element in a Network

Enclosed are:

- [x] 32 pages of specification, claims and abstract.
- [x] 6 sheets of [x] informal [ ] formal drawing(s).
- [x] A declaration and power of attorney.
- [x] An assignment transmittal.
- [x] An assignment of the invention to: RoamPage, Inc.  
Please record the assignment and return to the undersigned.
- [ ] A certified copy of a \_\_\_\_\_ application.
- [ ] An associate power of attorney.
- [x] A verified statement to establish small entity status under 37 CFR §§ 1.9 and 1.27.
- [ ] PTO Form-1449 and copies of cited art.

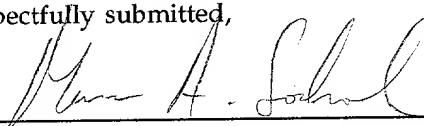
The filing fee has been calculated as shown below:

For	(Col. 1) No. Filed	(Col. 2) No. Extra	Small Entity		or	Other Than a Small Entity	
			Rate	Fee		Rate	Fee
Basic Fee				\$385.00			\$770.00
Total Claims	25- 20 =*	5	x \$11 =	\$55.00		x \$22 =	\$
Indep. Claims	7- 3 = *	4	x \$40 =	\$160.00		x \$80 =	\$
Multiple Dependent Claims Present [ ]			+ \$130 =	\$0.00		+ \$260 =	\$
*If the difference in column 1 is less than zero, enter 0 in column 2			Total	\$600.00	or	Total	\$

- [ ] Please charge my Deposit Account No. 06-0600 the amount of \$\_\_\_\_\_. A duplicate copy of this sheet is enclosed.
- [x] A check in the amount of \$640.00 to cover the filing fee [x] and recording of assignment is enclosed.
- [x] The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 06-0600. A duplicate copy of this sheet is enclosed.
  - [x] Any additional filing fees required under 37 CFR § 1.16.
  - [x] Any patent application processing fees under 37 CFR § 1.17.
  - [ ] The issue fee set in 37 CFR § 1.18 at or before mailing of the Notice of Allowance, pursuant to 37 CFR § 1.311(b).

Dated: 4/11/97

Respectfully submitted,

  
 Marc A. Sockol, Registration No. P-40,823  
 Carr, DeFilippo & Ferrell LLP  
 2225 East Bayshore Road, Suite 200  
 Palo Alto, California 94303  
 (415) 812-3407

SYSTEM AND METHOD FOR SECURELY SYNCHRONIZING MULTIPLE  
COPIES OF A WORKSPACE ELEMENT IN A NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

5        This application is related to co-pending patent application  
entitled "System and Method for Globally Accessing Computer  
Services," serial number 08/766,307, filed on December 13, 1996, by  
inventors Mark D. Riggins, R. Stanley Bailes, Hong Q. Bui, David J.  
Cowan, Daniel J. Mendez, Mason Ng, Sean Michael Quinlan, Prasad  
10      Wagle, Christine C. Ying, Christopher R. Zuleeg and Joanna A.  
Aptekar-Strober; and to co-pending patent application entitled  
"System and Method for Enabling Secure Access to Services in a  
Computer Network," serial number \_\_\_\_\_, filed on \_\_\_\_\_, by  
inventor Mark Riggins, both of which are hereby incorporated by  
15      reference. These related applications have been commonly assigned  
to RoamPage, Inc.

BACKGROUND OF THE INVENTION1. Field of the Invention

This invention relates generally to computer networks, and more particularly to a system and method for securely synchronizing 5 multiple copies of a workspace element such as a file in a secure network.

2. Description of the Background Art

Data consistency is a significant concern for computer users. 10 For example, when maintaining multiple independently-modifiable copies of a document, a user risks using an outdated version. Further, by the time the user notices the inconsistency, interparty miscommunication or data loss may have resulted. The user must then spend more time attempting to reconcile the inconsistent 15 versions.

The problem of data inconsistency is exacerbated when multiple copies of a document are maintained at different network locations. For example, due to network security systems such as conventional firewall technology, a user may have access only to a 20 particular one of these network locations. Without access to the other sites, the user cannot confirm that the version on the accessible site is the most recent draft.

Therefore, a system and method are needed for providing users with data consistency, and more particularly for synchronizing multiple copies of a workspace element such as a document in the secure network environment.

5

#### SUMMARY OF THE INVENTION

The present invention provides a system and method for synchronizing multiple copies of a workspace element in a secure network environment. The secure network environment includes a 10 global server connected to multiple clients. Using the present system and method, the clients automatically synchronize workspace data between multiple sites, independent of whether the sites are protected by site firewalls.

The present system includes a general synchronization module 15 at the client site for operating within a first firewall and for examining first version information to determine whether a first workspace element has been modified. The system further includes a synchronization agent at the global server for operating outside the first firewall and for forwarding to the general synchronization module second version information which indicates whether an 20 independently-modifiable copy of the first workspace element has been modified. A synchronization-start module at the client site

operates within the first firewall and initiates the general synchronization module and the synchronization agent when predetermined criteria have been satisfied. The system further includes means for generating a preferred version from the first 5 workspace element and from the copy by comparing the first version information and the second version information, and means for storing the preferred version at the first store and at the second store.

The system further handles the case when both the workspace 10 element and the copy have been modified independently since the last date and time of synchronization. Accordingly, a content-based synchronization module performs a responsive action such as determined a preferred version or storing both the first workspace element and the copy at both the first store and at the second store.

15 The present method includes the steps of generating first examination results by examining first version information, which indicates whether a first workspace element stored at a first store within a firewall has been modified; and generating second examination results by examining second version information which 20 indicates whether an independently-modifiable copy of the first workspace element, the copy being stored at a second store outside the firewall, has been modified. The present method further

includes the steps of initiating synchronization from within the firewall when predetermined criteria have been satisfied; generating a preferred version from the first workspace element and from the copy based on the first and second examination results; and storing 5 the preferred version at the first store and at the second store.

The system and method advantageously use a trusted third party to enable the synchronization of workspace data among multiple sites. Accordingly, a client user who maintains a work site, a home site, an off-site and the global server site can synchronize the 10 workspace data or portions thereof among all four sites. Further, the predetermined criteria (which controls when the synchronization-start module initiates synchronization) may be set so that the general synchronization module synchronizes the workspace data upon user request, at predetermined times during the day such as while the 15 user is commuting, or after a predetermined user action such as user log-off or user log-on. Because the system and method operate over the Internet, synchronization can occur over any distance. Since synchronization is initiated from within the firewall, the typical 20 firewall, which prevents in-bound communications, does not act as an impediment to workspace data synchronization. Also, since the user's preferences may be previously set, the present system and method may operate unattended by the client user.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a secure data-synchronizing network in accordance with the present invention;

FIG. 2 is a block diagram illustrating details of a FIG. 1 service  
5 server;

FIG. 3 is a block diagram illustrating details of the FIG. 1  
desktop computer;

FIG. 4 is a block diagram illustrating details of the FIG. 3 base  
system;

10 FIG. 5 is a block diagram illustrating details of the FIG. 1  
synchronization agent; and

FIG. 6 is a flowchart illustrating a method for synchronizing  
multiple copies of a workspace element in a secure network.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 is a block diagram illustrating a secure data-synchronizing network 100, comprising a first site such as a remote computer terminal 105 coupled via a communications channel 110 such as the Internet to a global server 120. The global server 120 is 5 in turn coupled via a communications channel 125 such as the Internet to a second site such as a corporate Local Area Network (LAN) 135. The global server 120 is protected by a global firewall 115, and the corporate LAN 135 is protected by a corporate firewall 10 130.

The corporate LAN 135 includes a corporate signal bus 140 coupling the corporate firewall 130 to an e-mail server 145 having e-mail data 165, to a file server 150 having file data 170, to a calendar server 155 having calendar data 175 and to a desktop 15 computer 160 having user data 180. It will be appreciated that the e-mail data 165, file data 170, calendar data 175 and user data 180 or portions thereof may be stored at different locations such as locally on the desktop computer 160. It will be further appreciated that the e-mail data 165, file data 170, calendar data 175 and user 20 data 180 are exemplary and collectively referred to herein as "workspace data" 185. Those skilled in the art will recognize that "workspace data" may include other types of data such as

application programs. It will be further appreciated that the e-mail data 165, file data 170, calendar data 175 and user data 180 may each be divided into workspace elements, wherein each workspace element is identified by particular version information 255 (described below with reference to FIG. 2). Accordingly, each e-mail, file, calendar, etc. may be referred to as "a workspace element in workspace data."

An independently modifiable copy of the workspace data 185, referred to herein as workspace data 123, is stored on the global server 120 for easy access by a user from the remote terminal 105. Being a copy, the workspace data 123 includes independently modifiable copies of each workspace element in workspace data 185 and an independently modifiable copy of version information 255 (FIG. 2), referred to herein as version information 124.

Network 100 further comprises synchronization means, which includes a base system 190 stored within the corporate LAN 135 and for example on the desktop computer 160 and further includes a synchronization agent 126 stored outside the corporate firewall 130 and preferably on the global server 120. The base system 190 and the synchronization agent 126 cooperate to synchronize the workspace data 185 with the workspace data 123. Generally, the base system 190 manages the workspace data 185 within the

corporate LAN 135 and the synchronization agent 126 manages the workspace data 123 within the global server 120. As described in greater detail below with reference to FIG. 4, the base system 190 preferably initiates and controls data synchronization. Other 5 components and functions of the global server 120 are described in the cross-referenced patent applications which are herein incorporated by reference.

The remote terminal 105 may include a smart telephone or a Personal Data Assistant (PDA) such as the PalmPilot system by the 10 U.S. Robotics, Inc. Although not shown, the remote terminal 105 may include a second base system similar to the base system 190, which is described with greater detail with reference to FIG. 4. Accordingly, the second base system on the remote terminal 105 would cooperate with the synchronization agent 126 to synchronize 15 the workspace data stored on the remote terminal 105 with the workspace data 123 stored on the global server 120. As with the corporate LAN, the second base system on the remote terminal 105 would preferably initiate and control data synchronization with the global server 120 for the same reasons discussed below. Workspace 20 data on the remote terminal 105 would thus be synchronized with the workspace data 123 and with the workspace data 185,

FIG. 2 is a block diagram illustrating details of a service server 200, wherein each of the e-mail server 145, the file server 150, the calendar server 155 and the desktop computer 160 is an instance 5 thereof. Service server 200 includes a Central Processing Unit (CPU) 205 such as a Motorola Power PC® microprocessor or an Intel Pentium® microprocessor. An input device 210 such as a keyboard and mouse and an output device 215 such as a Cathode Ray Tube (CRT) display are coupled via a signal bus 220 to CPU 205. A 10 communications interface 225 (such as an Ethernet port), a data storage device 230 (such as read only memory or a magnetic disk), and Random-Access Memory (RAM) 235 are further coupled via signal bus 220 to the CPU 205.

An operating system 240 includes a program for controlling 15 processing by the CPU 205, and is typically stored in the data storage device 230 and loaded into the RAM 235 for execution. A service engine 245 includes a program for performing a particular service such as maintaining an e-mail data base, a calendar data base, a bookmarks data base or another file data base, and may be also 20 stored in the data storage device 230 and loaded into the RAM 235 for execution. To perform a service, the service engine 245 operates on service data 250 (e.g., the e-mail data 165, the file data 170, the

calendar data 175 or the user data 180), which is typically stored in the data storage device 250. The service data 250 includes version information 255 indicating the date and time of the last modification. The service engine 245 operates to update the version information 5 255 whenever modifications are made. It will be appreciated that the portion of memory in the data storage device 250 which contains the service data 250 is referred to as the service “store.”

FIG. 3 is a block diagram illustrating details of the desktop 10 computer 160, which includes a CPU 305, an input device 310, an output device 315, a communications interface 325, a data storage device 330 and RAM 335, each coupled to a signal bus 320.

An operating system 340 includes a program for controlling processing by the CPU 305, and is typically stored in the data storage 15 device 330 and loaded into the RAM 335 for execution. A desktop service engine 345 (i.e., a particular service engine 245, FIG. 2) includes a service program for managing user data 180 (i.e., particular service data 250, FIG. 2) which includes version information 350 (i.e., particular version information 255, FIG. 2). The 20 desktop service engine 345 may be also stored in the data storage device 330 and loaded into the RAM 335 for execution. The user data 180 may be stored in the data storage device 330. As stated

above with reference to FIG. 1, the base system 190 operates to synchronize the workspace data 185 (which includes user data 180) with the workspace data 123. The base system 190 may be also stored in the data storage device 330 and loaded into the RAM 335 5 for execution.

FIG. 4 is a block diagram illustrating details of the base system 190, which includes a communications module 405, a user interface module 410, a locator module 415, a synchronization-start (“synch-start”) module 420, a general synchronization module 425 and a content-based synchronization module 430. For simplicity, each module is illustrated as communicating with one another via a signal bus 440.

The communications module 405 includes routines for compressing data, and routines for communicating via the communications interface 325 (FIG. 3) with the synchronization agent 126 (FIG. 1). The communications module 405 may further include routines for applying Secure Socket Layer (SSL) technology and user identification and authentication techniques (i.e., digital certificates) to establish a secure communication channel through the corporate firewall 130 and through the global firewall 126.

Examples of communications modules 405 may include TCP/IP stacks or the AppleTalk® protocol.

The user interface 410 includes routines for communicating with a user, and may include a conventional Graphical User Interface (GUI). The user interface 410 operates in coordination with the other desktop computer 160 components as described herein.

The locator module 415 includes routines for identifying the memory locations of the workspace elements in the workspace data 185 and the memory locations of the workspace elements in the workspace data 123. Workspace element memory location identification may be implemented using intelligent software, i.e., preset memory addresses or the system's registry, or using dialogue boxes to query a user. Accordingly, the locator module 415 determines the memory addresses of the workspace elements in the e-mail data 165, the workspace elements in the file data 170, the workspace elements in the calendar data 175 and the workspace elements in the user data 180 as well as the memory addresses of the corresponding workspace elements in the workspace data 123. It will be appreciated that the locator module 415 may perform workspace element memory location identification upon system boot-up or after each communication with the global server 120 to maintain updated memory locations of workspace elements.

The synchronization-start module 420 includes routines for determining when to initiate synchronization of workspace data 123 and workspace data 185. For example, the synchronization-start module 420 may initiate data synchronization upon user request, at 5 a particular time of day, after a predetermined time period passes, after a predetermined number of changes, after a user action such as user log-off or upon like criteria. The synchronization-start module 420 initiates data synchronization by instructing the general synchronization module 425 to begin execution of its routines. It will 10 be appreciated that communications with synchronization agent 126 preferably initiate from within the corporate LAN 1135, because the typical corporate firewall 130 prevents in-bound communications and allows out-bound communications.

The general synchronization module 425 includes routines for 15 requesting version information 124 from the synchronization agent 126 (FIG. 1) and routines for comparing the version information 255 against a last synchronization signature 435 such as a last synchronization date and time to determine which versions have been modified. The general synchronization module 425 further 20 includes routines for comparing the version information 124 and the version information 255 to determine if only one or both versions of a particular workspace element have been modified and routines for

performing an appropriate synchronizing responsive action.

Appropriate synchronizing responsive actions may include forwarding the modified version (as the preferred version) of a workspace element in workspace data 185 or forwarding just a 5 compilation of the changes to the other store(s). Other appropriate synchronizing responsive actions may include, if reconciliation between two modified versions is needed, then instructing the content-based synchronization module 430 to execute its routines which are described below.

10 It will be appreciated that the synchronization agent 126 preferably examines the version information 124 and forwards only the version information 124 determined to be modified since the last synchronization signature 435. This technique makes efficient use of processor power and avoids transferring unnecessary data across the 15 communications channel 125. The general synchronization module 425 in the corporate LAN 135 accordingly compares the received version information 124 with the version information 255 to determine if reconciliation is needed. Upon completion of the data synchronization, the general synchronization module 425 updates the 20 last synchronization signature 435.

The content-based synchronization module 430 includes routines for reconciling two or more modified versions in workspace

data 123, 185 of the same workspace element. For example, if the original and the copy of a user workspace element have both been modified independently since the last synchronization, the content-based synchronization module 430 determines the appropriate 5 responsive action. The content-based synchronization module 430 may request a user to select the preferred one of the modified versions or may respond based on preset preferences, i.e., by storing both versions in both stores or by integrating the changes into a single preferred version which replaces each modified version at 10 both stores.

FIG. 5 is a block diagram illustrating details of the synchronization agent 126, which includes a communications module 505 (similar to the communications module 405 described above 15 with reference to FIG. 4) and a general synchronization module 510 (similar to the general synchronization module 425 described above also with reference to FIG. 4). The communications module 505 includes routines for compressing data, and routines for 20 communicating via the communications channel 125 with the base system 190. The communications module 505 may further include routines for establishing a secure communications channel through the global firewall 126 and through the corporate firewall 130.

The general synchronization module 510 includes routines for comparing the version information 124 with the last synchronization signature 435, and routines for forwarding to the general synchronization module 425 version information 124 determined to 5 be modified. The general synchronization module 510 may either maintain its own last synchronization signature 435 copy (not shown). Alternatively, the request to synchronize from the base system 190 may include a copy of the last synchronization signature 435. The general synchronization module 510 further includes 10 routines for receiving preferred versions of workspace data 185 workspace elements from the general synchronization module 425, and routines for forwarding preferred versions of workspace data 123 workspace elements to the general synchronization module 425.

15 FIG. 6 is a flowchart illustrating a method 600 for synchronizing multiple copies of workspace data 123, 185 in a secure network 100. Method 600 begins with locator module 415 in step 605 identifying the memory locations of the workspace elements in workspace data 123, 185. As stated above, workspace element 20 memory location identification may be implemented using intelligent software or dialogue boxes. The user interface module 410 in step 610 enables selection of the workspace elements in workspace data

123, 185 to be synchronized by the general synchronization module 425.

The synchronization-start module 420 in step 615 determines whether predetermined criteria have been met which indicate that 5 synchronization of the workspace elements selected in step 610 should start. If not, then method 600 loops back to step 615.

Otherwise, the communications module 405 and communications module 505 in step 617 establish a secure communications channel between the global server 120 and the desktop computer 160. The 10 general synchronization module 510 in step 620 compares the version information 124 of each of the selected workspace elements in workspace data 123 against the last synchronization signature 435 to determine modified workspace elements, and forwards the version information 124 of workspace elements determined to be 15 modified to the general synchronization module 425. Further, the general synchronization module 425 in step 620 compares the version information 255 of each selected workspace element in the workspace data 185 against the last synchronization signature 435 to locate modified workspace elements. In this embodiment, a 20 workspace element has been modified if the date and time of last modification is after the date and time of last synchronization.

If no modified workspace elements in workspace data 123 or in workspace data 185 are located, then the general synchronization modules 425 and 510 in step 650 update the last synchronization signature 435 and method 600 ends. Otherwise, the general 5 synchronization module 425 in step 625 determines whether more than one version of the same workspace element has been modified since the last synchronization.

If only one version has been modified, then the corresponding general synchronization module 425 or 510 in step 630 forwards the 10 updated preferred version of the workspace element to the other store, and then in step 635 determines whether all workspace elements selected in step 610 have been examined. If so, then method 600 jumps to step 650. Otherwise, then method 600 returns to step 620.

15 If more than one version has been modified, then the general synchronization module 425 in step 640 instructs the content-based synchronization module 430 to reconcile the modified versions. Reconciliation may include requesting instructions from the user or, based on preselected preferences, performing responsive actions 20 such as storing both versions at both stores.

General synchronization module 425, 510 in step 645 sends the preferred version of the workspace element or just a compilation of

the changes to the other store. That is, if the preferred version is a workspace element in the workspace data 185, then general synchronization module 425 sends the preferred version or the changes to general synchronization module 510 to update the 5 outdated workspace element in the workspace data 123. If the preferred version is a workspace element in the workspace data 123, then the general synchronization module 510 sends the preferred version or the changes to the general synchronization module 425 to update the outdated workspace element in the workspace data 185. 10 Method 600 then jumps to step 635.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the 15 present invention. For example, although the global server 120 is illustrated as a single device, the global server 120 may include several computers networked together. Although not described in great detail, the remote terminal 105 can synchronize copies of workspace elements stored on it with workspace elements of 20 workspace data 123 stored on the global server 120. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated

circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

WHAT IS CLAIMED IS:

1 1. A computer-based method comprising the steps of:  
2 (a) generating first examination results from first version  
3 information which indicates whether a first workspace element  
4 stored at a first store within a firewall has been modified;  
5 (b) generating second examination results from second version  
6 information which indicates whether an independently-modifiable  
7 copy of the first workspace element has been modified, the copy  
8 being stored at a second store outside the firewall;  
9 (c) initiating steps (a) and (b) from within the firewall when  
10 predetermined criteria have been satisfied;  
11 (d) generating a preferred version from the first workspace  
12 element and from the copy based on the first and second  
13 examination results; and  
14 (e) storing the preferred version at the first store and at the  
15 second store.

1 2. The method of claim 1 wherein the second store is on a global  
2 server outside the firewall and which is protected by a global  
3 firewall.

1 3. The method of claim 1 wherein the first version information  
2 includes the date and time the first workspace element was last  
3 modified and the second version information includes the date and  
4 time the copy was last modified.

1 4. The method of claim 3 wherein generating the first  
2 examination results includes the step of comparing the first version  
3 information against a date and time of last synchronization.

1 5. The method of claim 3 wherein generating the second  
2 examination results includes the step of comparing the second  
3 version information against a date and time of last synchronization.

1 6. The method of claim 1 further comprising, before generating  
2 the first examination results, the step of updating the first version  
3 information whenever the first workspace element is modified.

1 7. The method of claim 1 further comprising, before generating  
2 the second examination results, the step of updating the second  
3 version information whenever the copy is modified.

1 8. The method of claim 1 wherein if only one of the first  
2 workspace element and the copy has been modified, then the step of  
3 generating includes selecting the one as the preferred version.

1 9. The method of claim 1 further comprising the step of locating  
2 the first workspace element, the first version information, the copy  
3 and the second version information.

1 10. A system comprising:  
2 a general synchronization module for operating within a first  
3 firewall and for examining first version information to determine  
4 whether a first workspace element has been modified;  
5 a synchronization agent for operating outside the first firewall  
6 and for forwarding to the general synchronization module second  
7 version information which indicates whether an independently-  
8 modifiable copy of the first workspace element has been modified;  
9 a synchronization-start module for operating within the first  
10 firewall and for initiating the general synchronization module and  
11 the synchronization agent when predetermined criteria have been  
12 satisfied;

13       means for generating a preferred version from the first  
14   workspace element and from the copy by comparing the first version  
15   information and the second version information; and  
16       means for storing the preferred version at the first store and at  
17   the second store.

1   11. The system of claim 10 further comprising a communications  
2   module for communicating through the first firewall.

1   12. The system of claim 10 wherein the synchronization agent and  
2   the second store are on a global server which is protected by a global  
3   firewall.

1   13. The system of claim 12 further comprising a communications  
2   module for communicating through the first firewall and through the  
3   global firewall.

1   14. The system of claim 10 wherein the first version information  
2   includes the date and time the first workspace element was last  
3   modified and the second version information includes the date and  
4   time the copy was last modified.

1 15. The system of claim 14 wherein the general synchronization  
2 module compares the first version information against a date and  
3 time of last synchronization.

1 16. The system of claim 14 wherein the synchronization agent  
2 compares the second version information against the date and time  
3 of last synchronization.

1 17. The system of claim 10 further comprising means for updating  
2 the first version information whenever the first workspace element  
3 is modified.

1 18. The system of claim 10 further comprising means for updating  
2 the second version information whenever the copy is modified.

1 19. The system of claim 10 wherein if only one of the first  
2 workspace element and the copy has been modified, then the means  
3 for generating selects the one as the preferred version.

1 20. The system of claim 10 further comprising a locator module for  
2 locating the first store, the first workspace element, the first version  
3 information, the second store, the copy and the second version  
4 information.

1 21. A system comprising:  
2       first means for generating first examination results from first  
3 version information which indicates whether a first workspace  
4 element stored at a first store within a firewall has been modified;  
5       second means for generating second examination results from  
6 second version information which indicates whether an  
7 independently-modifiable copy of the first workspace element has  
8 been modified, the copy being stored at a second store outside the  
9 firewall;  
10      means for initiating the first and second means from within the  
11 firewall when predetermined criteria have been satisfied;  
12      means for generating a preferred version from the first  
13 workspace element and from the copy based on the first and second  
14 examination results; and  
15      means for storing the preferred version at the first store and at  
16 the second store.

1 22. A computer-readable storage medium storing program code for  
2 causing a computer to perform the steps of:  
3 (a) generating first examination results from first version  
4 information which indicates whether a first workspace element  
5 stored at a first store within a firewall has been modified;  
6 (b) generating second examination results from second version  
7 information which indicates whether an independently-modifiable  
8 copy of the first workspace element has been modified, the copy  
9 being stored at a second store outside the firewall;  
10 (c) initiating steps (a) and (b) from within the firewall when  
11 predetermined criteria have been satisfied;  
12 (d) generating a preferred version from the first workspace  
13 element and from the copy based on the first and second  
14 examination results; and  
15 (e) storing the preferred version at the first store and at the  
16 second store.

1 23. A computer-based method comprising the steps of:

2 (a) generating first examination results from first version

3 information which indicates whether a first workspace element

4 stored at a first store within a firewall has been modified;

5 (b) generating second examination results from second version

6 information which indicates whether an independently-modifiable

7 copy of the first workspace element has been modified, the copy

8 being stored at a second store outside the firewall;

9 (c) initiating steps (a) and (b) from within the firewall when

10 predetermined criteria have been satisfied;

11 (d) determining based on the first and second examination results

12 that both the first workspace element and the copy have been

13 modified; and

14 (e) storing both the first workspace element and the copy at the

15 first store and at the second store.

1 24. A system comprising:

2 first means for generating first examination results from first  
3 version information which indicates whether a first workspace  
4 element stored at a first store within a firewall has been modified;

5 second means for generating second examination results from  
6 second version information which indicates whether an  
7 independently-modifiable copy of the first workspace element has  
8 been modified, the copy being stored at a second store outside the  
9 firewall;

10 means for initiating the first and second means from within the  
11 firewall when predetermined criteria have been satisfied;

12 means for determining based on the first and second  
13 examination results that both the first workspace element and the  
14 copy have been modified; and

15 means for storing both the first file and the copy at the first  
16 store and at the second store.

1 25. A system comprising:

2       a global server for operating outside a firewall and including

3               memory for storing first workspace data and

4               corresponding first version information; and

5               a synchronization agent for managing the first workspace

6        data and the corresponding first version information and for

7        communicating with remote clients; and

8        a remote client for operating within the firewall and including

9               memory for storing second workspace data and

10          corresponding second version information;

11               means for cooperating with the synchronization agent to

12        synchronize the first workspace data with the second

13        workspace data by examining the first version information and

14        the second version information; and

15               a synchronization-start module for initiating workspace

16        data synchronization between the global server and the remote

17        client.

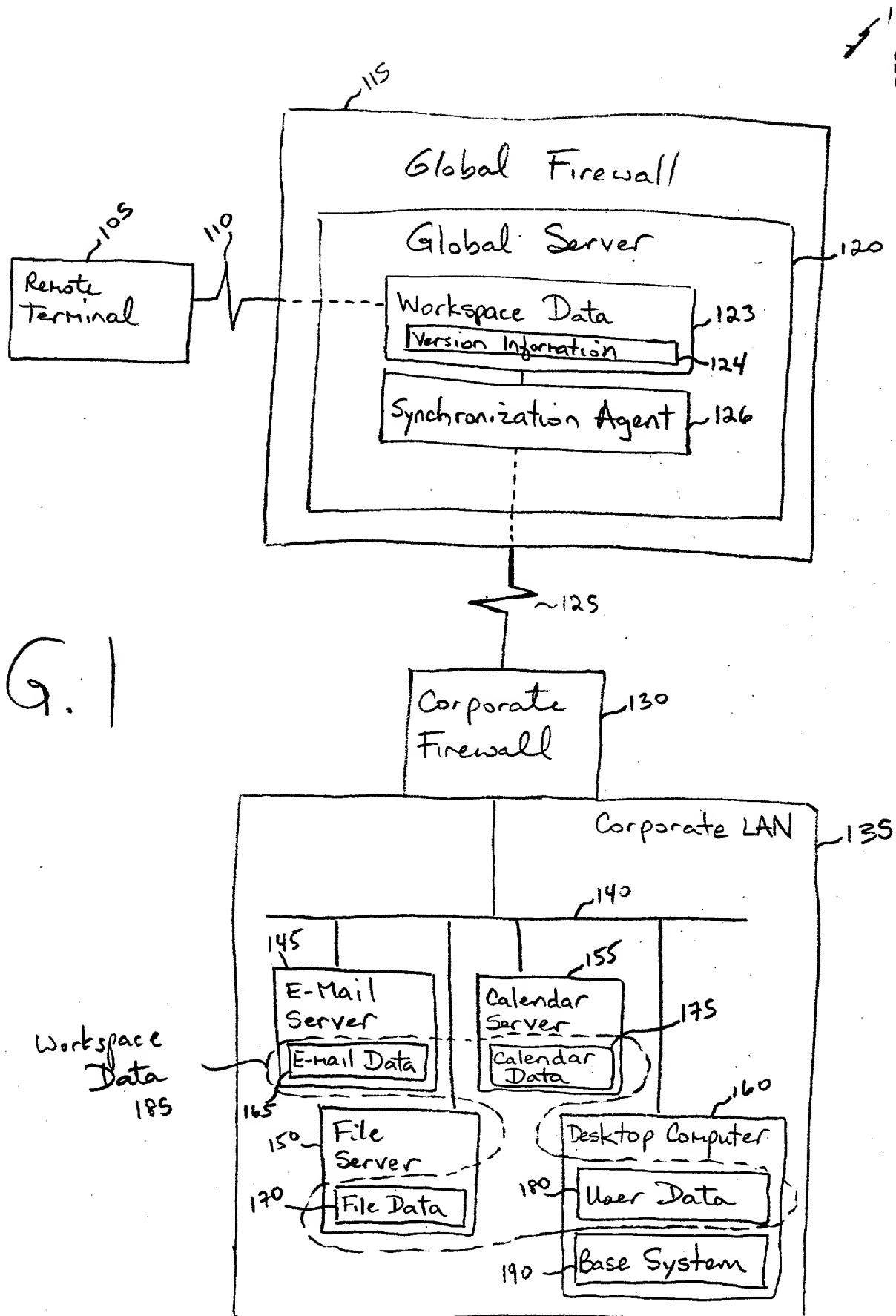
SYSTEM AND METHOD FOR SECURELY SYNCHRONIZING MULTIPLE  
COPIES OF A WORKSPACE ELEMENT IN A NETWORK

ABSTRACT OF THE DISCLOSURE

5       A system includes a general synchronization module at the client site for operating within a first firewall and for examining first version information to determine whether a first workspace element has been modified. The system further includes a synchronization agent at a global server for operating outside the first firewall and 10 for forwarding to the general synchronization module second version information which indicates whether an independently-modifiable copy of the first workspace element has been modified. A synchronization-start module is maintained at the client site for operating within the first firewall and for securely initiating the 15 general synchronization module and the synchronization agent when predetermined criteria have been satisfied. The system further includes means for generating a preferred version from the first workspace element and from the copy by comparing the first version information and the second version information, and means for 20 storing the preferred version at the first store and at the second store.

100  
69665 U.S. PTO  
08835749  
04/11/97  


FIG. 1



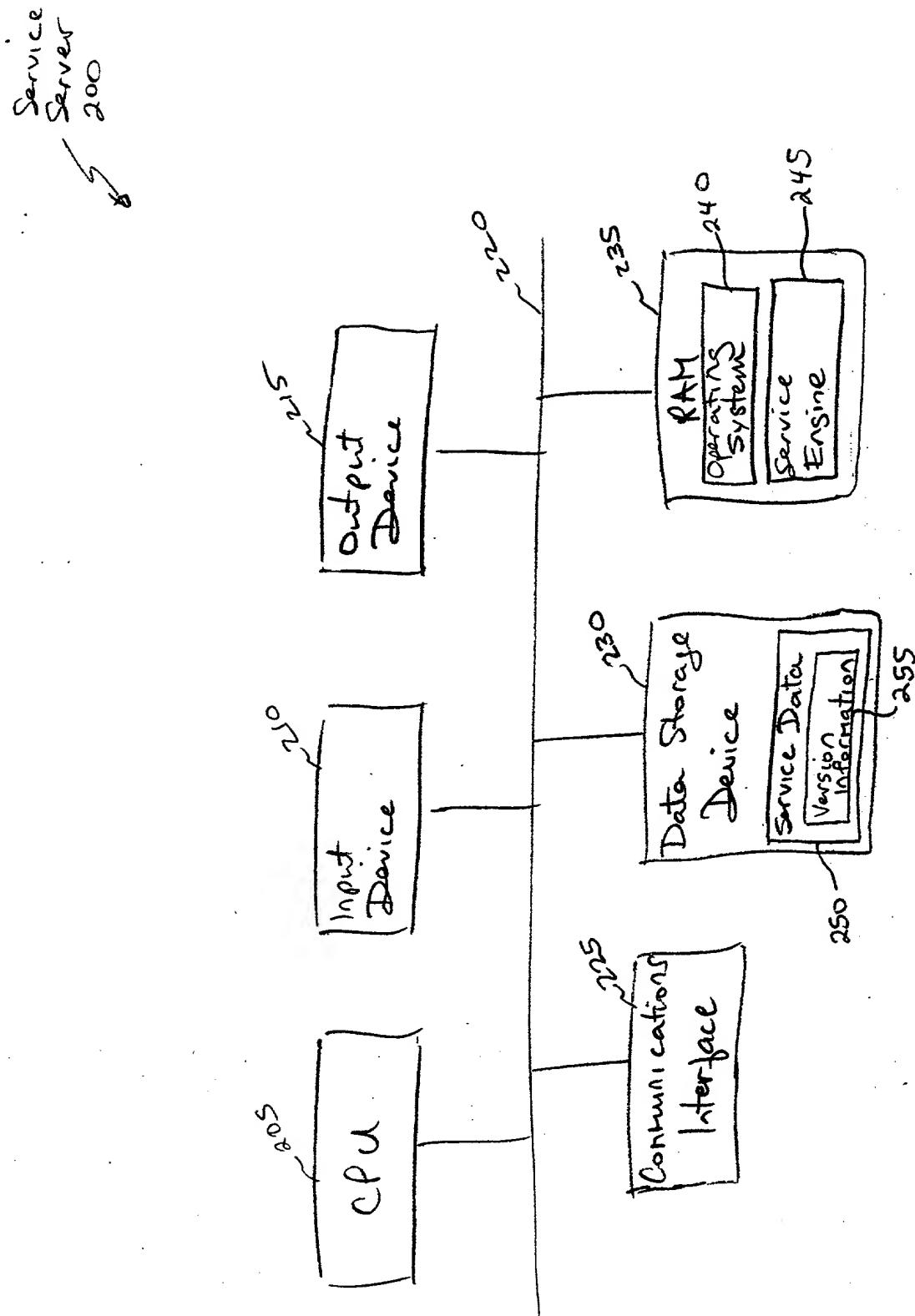


Fig. 2

Desktop Computer  
160

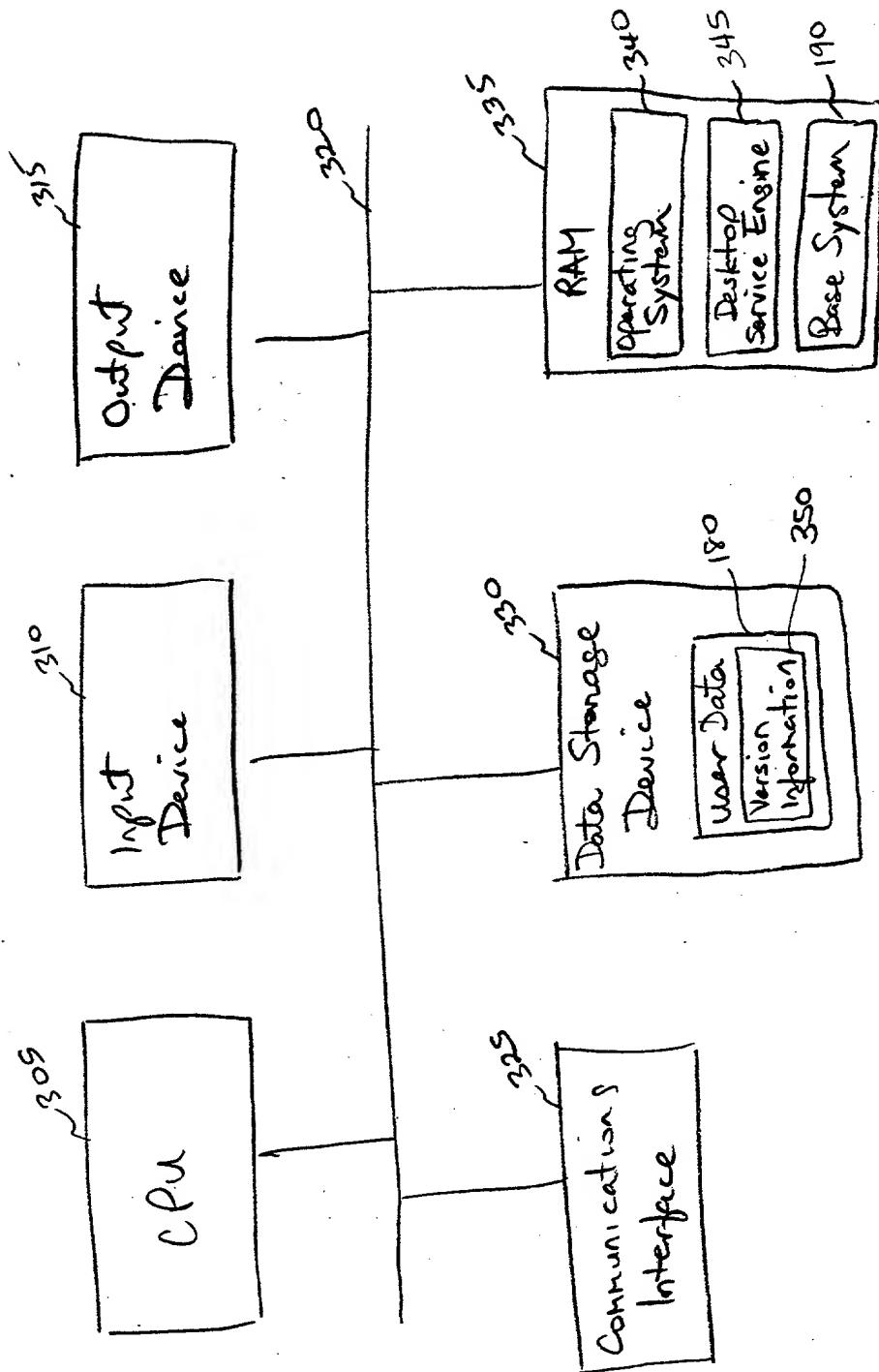
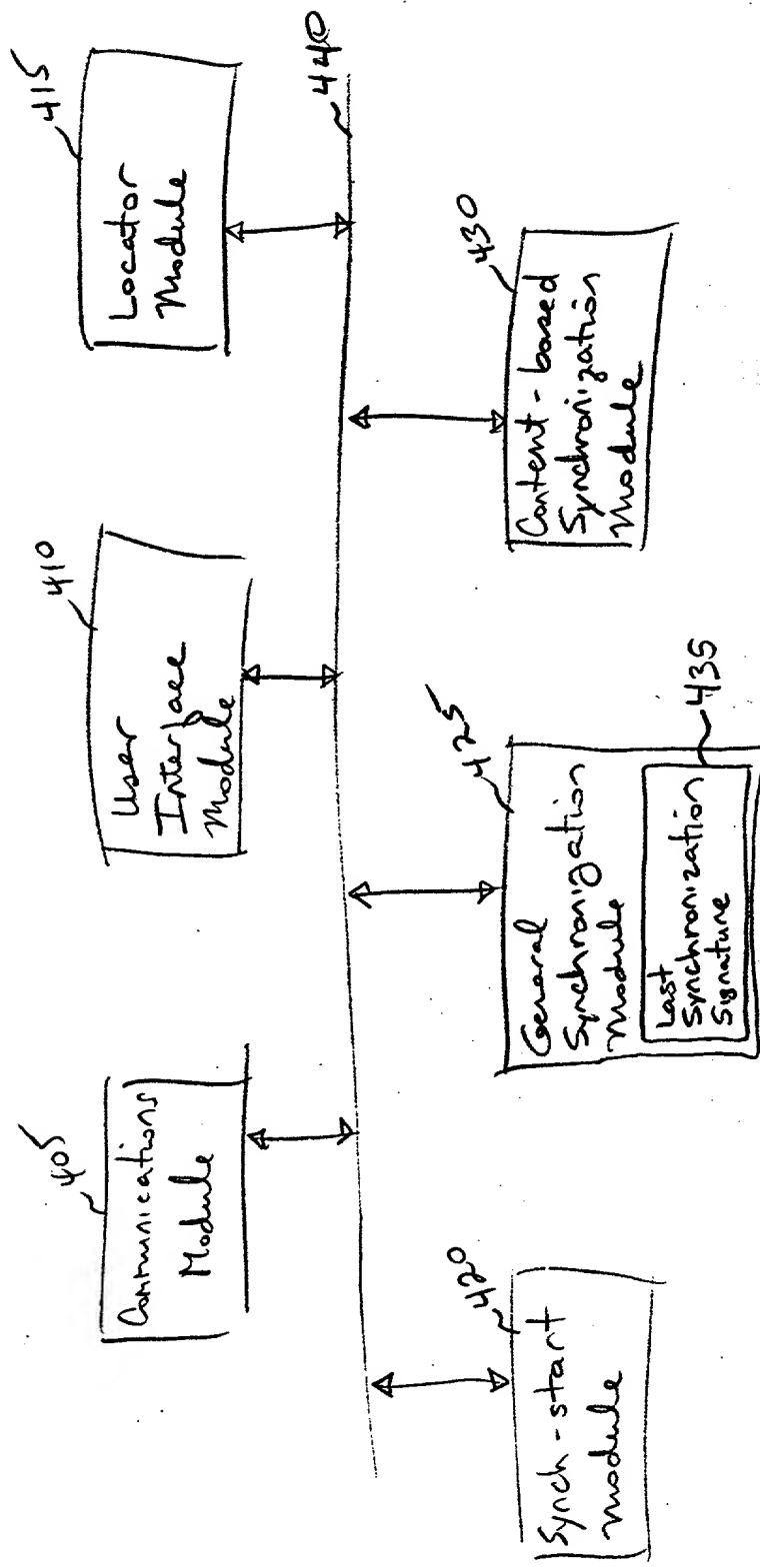


FIG. 3

Base  
System  
190



F | G | H

Synchronization  
Agent  
126

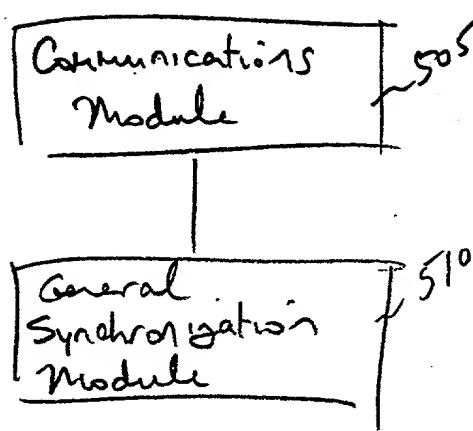
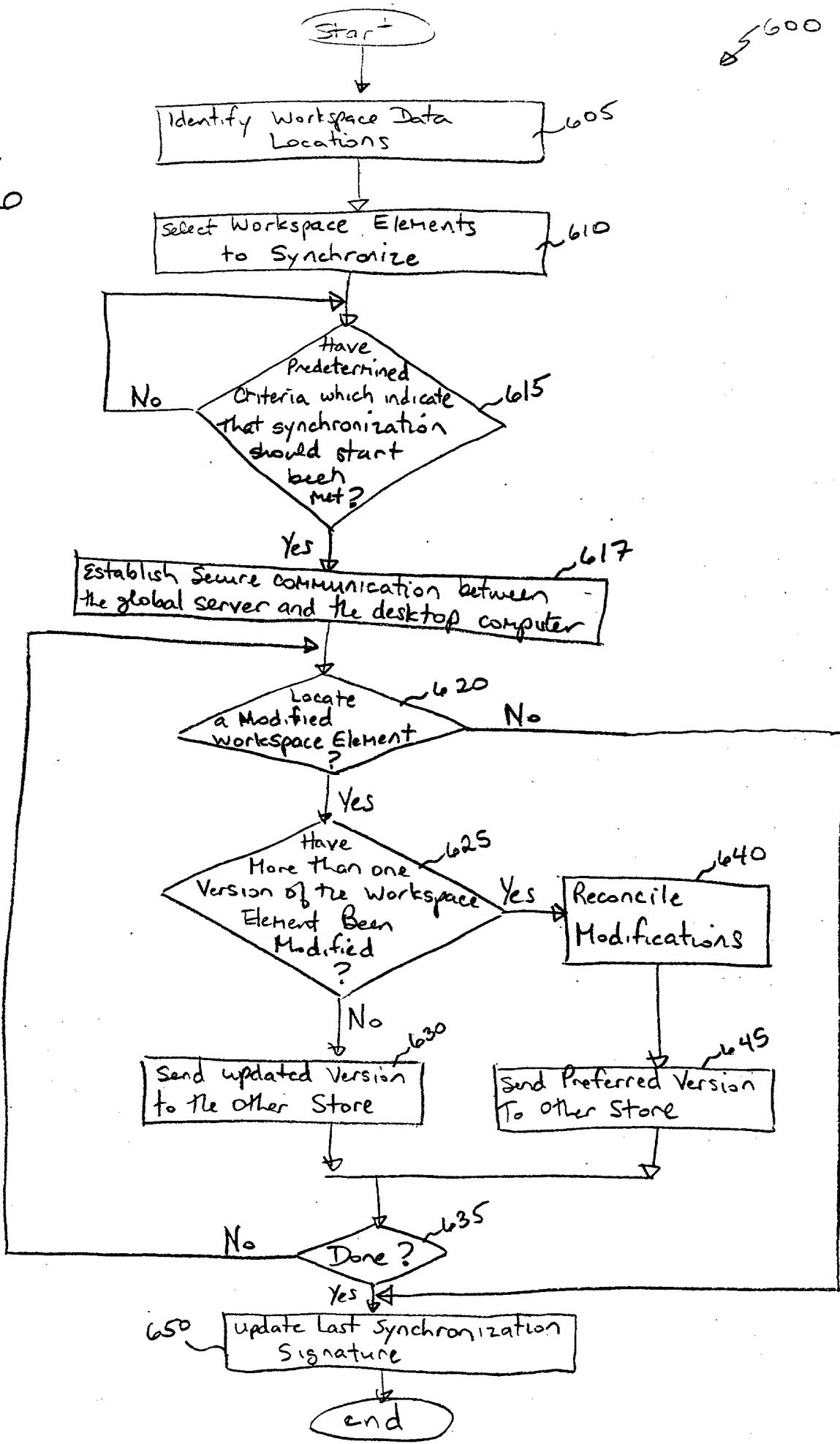


FIG. S

FIG. 6



ATTORNEY'S DOCKET NO.: 647

## DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled "System and Method for Securely Synchronizing Multiple Copies of a Workspace Element in a Network," the specification of which (check one):

is attached hereto.

was filed on \_\_\_\_\_ as U.S. Application No.  
or PCT International Application No. \_\_\_\_\_  
and was amended on \_\_\_\_\_ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed.

<u>Prior Foreign Application(s)</u>		<u>Priority Claimed</u>		
<u>(Number)</u>	<u>(Country)</u>	<u>(Day/Month/Year Filed)</u>	<u>Yes</u>	<u>No</u>
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

I hereby claim the benefit under Title 35, United States Code §119(e) of any United States provisional application(s) listed below.

---

(Application Number)

---

(Filing Date)

---

(Application Number)

---

(Filing Date)

I hereby claim the benefit under Title 35, United States Code §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

---

(Application Number)

---

(Filing Date)

---

(Status - patented, pending, abandoned)

---

(Application Number)

---

(Filing Date)

---

(Status - patented, pending, abandoned)

**POWER OF ATTORNEY:** I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

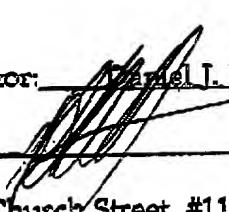
John S. Ferrell, Reg. No. 34,593; J. Eppa Hite, Reg. No. 30,266;  
Leroy D. Maunu Reg. No. 35,274; Francis H. Lewis, Reg. No. 27,684;  
Marc A. Sockol, Reg. No. P-40,823 and Gregory J. Koerner, Reg. No. 38,519

**SEND ALL CORRESPONDENCE TO:**

Marc A. Sockol  
CARR, DEFILIPPO & FERRELL LLP  
2225 East Bayshore Road, Suite 200  
Palo Alto, CA 94303  
TEL: (415) 812-3407  
FAX: (415) 812-3444

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

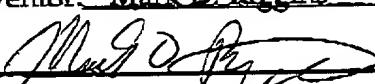
Full name of first inventor: Daniel J. Mendez

Inventor's signature  Dated: 4/11/97

Residence 801 Church Street, #1121, Mountain View, CA 94041

Post Office Address same Citizenship USA

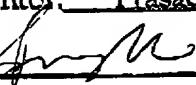
Full name of second inventor: Mark D. Riggins

Inventor's signature  Dated: 4-11-97

Residence 5818 Moraga Avenue, San Jose, CA 95123

Post Office Address same Citizenship USA

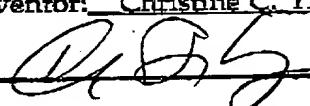
Full name of third inventor: Prasad Wagle

Inventor's signature  Dated: 4-11-97

Residence 2831 Pruneridge Avenue, Santa Clara, CA 95051

Post Office Address same Citizenship India

Full name of fourth inventor: Christine C. Ying

Inventor's signature  Dated: 4-11-97

Residence 1204 Moonsail Lane, Foster City, CA 94404

Post Office Address same Citizenship USA

Atty. Dkt.No. 647

Applicant: Daniel J. Mendez, et al.  
Serial or Patent No.: Unknown  
Filed or Issued: Herewith  
For: System and Method for Securely Synchronizing Multiple Copies of a Workspace Element in a Network.

VERIFIED STATEMENT (DECLARATION) CLAIMING  
SMALL ENTITY STATUS  
(37 CFR 1.9 (f) and 1.27 (c)) - SMALL BUSINESS CONCERN

I hereby declare that I am:

the owner of the small business concern identified below:  
 an official of the small business concern empowered to  
act on behalf of the concern identified below:

NAME OF CONCERN RoamPage, Inc.

ADDRESS OF CONCERN 156 East Dana Street, Mountain View, CA 94041

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.2, and reproduced in 37 CFR 1.9 (d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled "System and Method for Securely Synchronizing Multiple Copies of a Workspace Element in a Network," by inventors Daniel J. Mendez et al. and described in

the specification filed herewith  
 application serial no.       , filed         
 patent no.       , issued

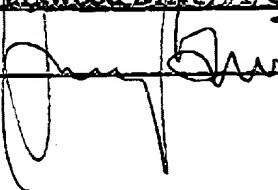
If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below\* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e). \*NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

NAME \_\_\_\_\_  
ADDRESS \_\_\_\_\_  
[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28 (b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of the Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING Hong O. Bui  
TITLE OF PERSON Vice President of Product Development  
ADDRESS 10250 Parkwood Drive, #4, Cupertino, CA 95014

SIGNATURE  DATE 4/11/97